STONESOFT

StoneGate SSL VPN Technical Note 2069

# Setting Up WPA Authentication

# Table of Contents

Introduction . . . . . page 3

Overview . . . . . page 3

How WPA Works . . . . . page 3

Setting Up WPA Authentication . . . . . page 4

Feedback . . . . . page 7

# Introduction

This technical note covers all aspects of the configuration of Wi-Fi Protected Access (WPA) Authentication for use with StoneGate SSL VPN.

## Prerequisites

This technical note assumes a thorough understanding of StoneGate SSL VPN administration and especially how wireless networks work. A basic understanding of OpenSSL is also required. Use the further reading to gain the required knowledge.

**Note –** Completing this procedure may require that the appliance is separately configured to accept connections from the external wireless access point. Contact Stonesoft support for instructions on how to do this.

## Further Reading

More information on StoneGate SSL VPN administration can be found in the *StoneGate SSL VPN Administrator's Guide*, the Online Help, and the Technical Note repository provided with the product. Another source of information is the Stonesoft Support site, which can be found at http://www.stonesoft.com/support/.

For more information on related subjects, visit

- http://www.wi-fi.org
- http://www.openssl.org

# Overview

StoneGate SSL VPN supports WPA authentication using a combination of 802.1X, which is a protocol for port-based network access control, and the Extensible Authentication Protocol (EAP). EAP is a general authentication protocol that supports multiple authentication methods, including traditional passwords, token cards, the Kerberos protocol, digital certificates, and public-key authentication.

WPA provides improved data encryption and user authentication using the Temporal Key Integrity Protocol (TKIP). Note that WPA requires the use of digital certificates.

In this solution, StoneGate authentication methods are used when logging on to a WLAN (wireless local area network). The authentication methods most suitable for use with WPA are StoneGate Synchronized and StoneGate Password. These authentication methods do not require more than a user name and a One-Time Password (OTP).

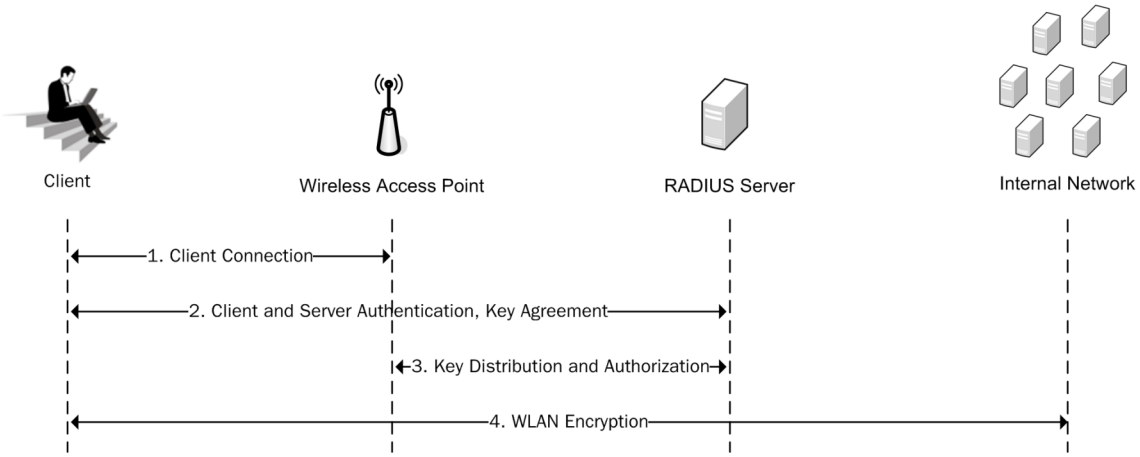
The RADIUS PEAP-MSCHAPv2 authentication protocol is used in the StoneGate SSL VPN WPA solution. This is built-in for Microsoft Windows XP and supported by many other platforms.

This technical note will guide you in setting up and configuring a WPA solution with StoneGate SSL VPN.

# How WPA Works

Communication using a 802.1X based network begins with a client device attempting to connect to the wire less access point. The wireless access point responds by enabling a port for passing EAP packets only from the client to the Authentication Service located on the wired side of the access point. The wireless access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the client's identity is verified by the Authentication Service (using RADIUS). Once authenticated, the wireless access point opens the client's port for traffic.

Illustration 1 Network communication




**Note –** The wireless access point can be provided by any Internet Service Provider (ISP), and it should not be confused with the StoneGate SSL VPN Access Point.

# Setting Up WPA Authentication

Setting up your StoneGate SSL VPN WPA authentication proceeds in the following order:

1. Create server certificate using OpenSSL, or use certificate generation batch file to generate a Certificate Authority (CA), certificate and a Server certificate. Instructions can be found in *Certificate Generation Batch File* on page 7.
2. Create database files for the CA
3. Create server extensions file
4. Sign server certificate with CA certificate using OpenSSL
5. Convert server private key using OpenSSL
6. Configure WPA authentication in StoneGate SSL VPN Administrator
7. Setup wireless access point to communicate with Authentication Service
8. Import CA certificate on Windows client
9. Setup Windows client to use PEAP-MSCHAPv2 authentication

These steps are outlined in detail below.

## Create CA Certificate

You will be using tools from OpenSSL to perform some of these steps. OpenSSL can be downloaded in the **Stonesoft Online and certificate request tools** section on the front page of the StoneGate SSL VPN Administrator. It is also possible to download OpenSSL from http:// www.openssl.org.

**Note –** Make sure you do not enter a Common Name and/or E-mail address for the CA certificate. This is a known issue that will be corrected in a future release.

By using OpenSSL commands, you will create a CA certificate that will expire in 10 years time. This CA certificate will be saved in the file ca.crt.

Use this OpenSSL command to prompt for CA certificate information. In this example, we use the password “anything”.

```
> openssl req -days 3652 -new -x509 -keyout ca.key -out ca.crt -passin
pass:anything -passout pass:anything
```

You can also use the certificate generation batch file to create the CA and server certificates. Instructions can be found in *Certificate Generation Batch File* on page 7.

## Create Server Certificate

A certificate request and a private key for the server certificate must also be created. The private key for this certificate will be saved in ca.key. Use this openSSL command to prompt for certificate information. Make sure to enter a “Common Name”, when prompted.

```
> openssl req -new -keyout server.key -out newreq.pem -passin pass:anything -
passout pass:anything
```

You can also use the certificate generation batch file to create the CA and server certificates. Instructions can be found in *Certificate Generation Batch File* on page 7.

## Create Database Files for the CA

OpenSSL needs some database files for holding the serial number and index list of issued certificates.
Use these DOS commands to create these database files:

```
> mkdir demoCA
> echo 01 > "demoCA\serial"
> echo # > "demoCA\index.txt"
```

## Create Server Extensions File

The extensions file contains the extensions that should be added to the server certificate when signing.
Edit file xpextensions and insert the following contents:

```
[ xpserver_ext ]
extendedKeyUsage = 1.3.6.1.5.5.7.3.1
```

Sign Server Certificate with CA Certificate Now we add the extensions defined in the previous step. The signed certificate will be output to server.crt. The certificate will be valid for 10 years.

```
> openssl ca -days 3652 -outdir . -cert ca.crt -keyfile ca.key -policy
policy_anything -out server.crt -passin pass:anything -key anything
-extensions xpserver_ext -extfile xpextensions -infiles newreq.pem
```

## Convert Server Private Key

We convert the server.key file into the PKCS8 format, which can be read by StoneGate SSL VPN Administrator. In this example, we give the private key the password “`anything`”.

```
> openssl pkcs8 -topk8 -in server.key -out server.pk8 -outform DER -passout
pass:anything -passin pass:anything
```

## Configure WPA Authentication in StoneGate SSL VPN Administrator

To complete your StoneGate SSL VPN WPA authentication, you need to configure the WPA authentication in StoneGate SSL VPN Administrator.

**▼To configure WPA authentication in StoneGate SSL VPN Administrator**

1. To import a CA Certificate, select **Manage System** in the main menu, and then click **Certificates** in the left-hand menu.
2. Click the **Add Certificate Authority** link.

3. Enter general settings.

**Example**

Display Name: `wpaCA`
CA Certificate: `ca.crt`

Revocation Control: `none`

4. Click **Next**.
5. Click **Finish Wizard**.
6. To import a server certificate, click the **Add Server Certificate** link.
7. Enter general settings.

**Example**

Display Name: `wpaServer`

Certificate: `server.crt`

Key: `server.pk8`

Password: `anything`

CA Certificate: `wpaCA`

8. Click **Save**.

The next step is to apply the server certificate.

**Note –** If you are using Revocation Control, then you have to do a few more changes.

## Apply Server Certificate

**▼To apply the server certificate for the Authentication Service**

1. Click **Authentication Services** in the left-hand menu.
2. In the **Registered Authentication Services** list, select applicable Authentication Service.
3. Select **Server Certificate**.

**Example**

`wpaServer`

4. Click **Save**.

The last step is to configure the RADIUS client.

## Configure RADIUS Client

**▼To configure the Access Point as a RADIUS client for the Authentication Service**

1. Click **RADIUS Configuration** in the left-hand menu.
2. Click the **Add RADIUS Client** link.
3. Enter general settings.

**Example**

`IP Address: <IP address of wireless access point>`

`Shared Secret: <shared secret>`

4. Click **Save**.
5. Click **Publish** to distribute changes to the StoneGate network.

## Setup Wireless Access Point to Communicate with Authentication Service

Configure your wireless access point as follows. Refer to the user manual for your wireless access point for details.

**▼To configure the wireless access point**

1. Configure IP address of Authentication Service.
2. Configure port to point out authentication method to use.

---

**Example**

`18123` (default) for StoneGate Password authentication

or

`18124` (default) for StoneGate Synchronized authentication

---

3. Set same shared secret as you did when you configured the wireless access point as RADIUS client for the Authentication Service in StoneGate SSL VPN Administrator.

---

**Note –** Completing this procedure may require that the appliance is separately configured to accept connections from the external wireless access point. Contact Stonesoft support for instructions on how to do this.

---

## Import CA Certificate on Windows Client

Double-click the CA certificate (ca.crt) and follow the wizard.

## Setup Windows Client to use PEAP-MSCHAPv2 Authentication

**▼To setup your Microsoft Windows client to use PEAP-MSCHAPv2 authentication**

1. Click **Start** and select **Control Panel** in the menu.
2. Double-click **Network Connections** to bring up the control panel for network configurations.
3. Right-click **Wireless Network Connection** and select **Properties**.
4. Click the **Wireless Networks** tab.
5. Select **Wireless Network** in the **Preferred networks** list.
6. Click **Properties**.
7. On the **Association** tab, enter **WPA** for Network Authentication.
8. On the **Authentication** tab, enter **Protected EAP (PEAP)** for EAP Type.
9. Click **Properties**.
10. Select **Secured Password (EAP-MSCHAPv2)** for **Authentication Method**.
11. Click **Configure**.
12. Deselect **Automatically use my Windows logon name and password**.
13. Click **OK** to finish the setup.

You are now ready to connect to the wireless network and authenticate yourself using your wireless network configuration.

## Certificate Generation Batch File

If you wish to generate a CA certificate and a server certificate at the same time, instead of using separate procedures, use the batch file. Remember to type all OpenSSL commands on one line.

# Feedback

Stonesoft is always interested in feedback from our users.

- For comments regarding Stonesoft's products, contact feedback@stonesoft.com.
- For comments regarding this technical note, contact documentation@stonesoft.com.

### Trademarks and Patents

Stonesoft, the Stonesoft logo and StoneGate are all trademarks or registered trademarks of Stonesoft Corporation. Multi-link technology, multi-link VPN, and the StoneGate clustering technology-as well as other technologies included in StoneGate-are protected by patents or pending patent applications in the U.S. and other countries. All other trademarks or registered trademarks are property of their respective owners.

SSL VPN Powered by PortWise

### Copyright and Disclaimer

Copyright © 2000–2010 Stonesoft Corporation. All rights reserved.

These materials, Stonesoft products and related documentation are protected by copyright and other laws, international treaties and conventions. All rights, title and interest in the materials, Stonesoft products and related documentation shall remain with Stonesoft and its licensors. All registered or unregistered trademarks in these materials are the sole property of their respective owners. No part of this document or related Stonesoft products may be reproduced in any form, or by any means without written authorization of Stonesoft Corporation.

Stonesoft provides these materials for informational purposes only. They are subject to change without notice and do not represent a commitment on the part of Stonesoft. Stonesoft assumes no liability for any errors or inaccuracies that may appear in these materials or for incompatibility between different hardware components, required BIOS settings, NIC drivers, or any NIC configuration issues. Use these materials at your own risk. Stonesoft does not warrant or endorse any third party products described herein.

THESE MATERIALS ARE PROVIDED "AS-IS." STONESOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO, THE INFORMATION CONTAINED HEREIN. IN ADDITION, STONESOFT MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT THE INFORMATION CONTAINED IN THESE MATERIALS.

IN NO EVENT SHALL STONESOFT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING FROM THE USE OF THESE MATERIALS, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

SG_SVTN_2069_20100416

STONESOFT

www.stonesoft.com

**Stonesoft Corporation**
Itälahdenkatu 22 A
FIN-00210 Helsinki
Finland
tel. +358 9 4767 11
fax +358 9 4767 1349

**Stonesoft Inc.**
1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338 USA
tel. +1 770 668 1125
fax +1 770 668 1131